問2　企業における情報セキュリティ管理に関する次の記述を読んで，設問 1～4 に答えよ。

X 社は，機械製品及び産業用資材の輸入及び国内販売業務を行う従業員数 1,000 名の商社であり，機械営業部，資材営業部，総務部，情報システム部などがある。

X 社は，数年前に同業他社で発生した情報セキュリティ事故を機に，情報セキュリティ管理に力を入れるようになり，JIS Q 27001 に基づく情報セキュリティマネジメントシステム（以下，X 社 ISMS という）を構築し，ISMS 認証を取得している。

X 社 ISMS では，副社長である最高情報セキュリティ責任者（CISO）を委員長とする情報セキュリティ委員会を設置し，各部の部長が情報セキュリティ委員会の委員を務めている。また，各部の部長は自部の情報セキュリティリーダを指名する。情報セキュリティ委員会は X 社 ISMS の年間活動計画を決定する。

X 社 ISMS の活動の実務は，各部の情報セキュリティリーダから構成される ISMS ワーキンググループ（以下，ISMS-WG という）が行っている。ISMS-WG のリーダは，情報システム部の S 課長である。ISMS-WG は，年間活動計画に基づき活動するほか，X 社 ISMS 規程などの文書（以下，X 社 ISMS 文書という）の改定案の検討を行う。

〔X 社 ISMS の年間活動計画〕

4 月のある日，今年度初めての ISMS-WG 会合が開催され，その席上で，表 1 に示す X 社 ISMS の年間活動計画が提示された。また，6 月に実施される情報資産目録の見直しについて S 課長から説明があった。X 社 ISMS では各部において情報資産の名称，管理責任者，重要度，保管場所，保管期間を記した情報資産目録を作成し，毎年見直すことになっている。しかし，毎年見直し後に幾つかの記載の過不足が見つかっていることから，見直し後の記載に過不足がないことをよく確認するよう，改めて S 課長が ISMS-WG のメンバに対して注意を促した。

表 1　X 社 ISMS の年間活動計画（抜粋）

時期	内容
5 月	ISMS-WG メンバ向け情報セキュリティ教育の実施
6 月	各部における①情報資産目録の見直し
8 月	全社を対象にした情報セキュリティリスクアセスメントの実施及びリスク対応計画の策定
12 月	従業員向け情報セキュリティ教育の実施
1 月	X 社 ISMS 規程の順守状況に関する内部監査の実施
3 月	情報セキュリティ委員会への年間活動報告及び情報セキュリティ委員会の審議事項の取りまとめ
随時 1)	情報セキュリティリスクアセスメントの実施及びリスク対応

注 1)　業務若しくは情報資産の大きな変更，又は情報セキュリティインシデントが発生した場合。

〔販路拡大のための施策〕

最近になって，主な取引先である海外の Y 社が，新製品として個人向けの 3D プリンタ（以下，3DP という）を開発した。これまで X 社は個人向けには製品を販売していなかったが，機械営業部では 3DP の個人向け販売を販路拡大の機会と捉え，そのための施策を検討した。その結果を表 2 に示す。

表 2　販路拡大のための施策

施策	内容
個人向け通信販売	インターネットを利用して，3DP の個人向け通信販売を行う。
X 社 Web サイトの改修	購入者が 3DP の関連情報を参照したり利用者登録をしたりできるよう，X 社 Web サイトを改修する。
SNS による情報提供	一般に広く使われている，短文の投稿及び写真の掲載が可能な SNS を利用し，新たに登録する X 社公式アカウントを通じて 3DP の使い方のコツ，ファームウェアの更新情報，利用事例などを紹介する。

機械営業部の情報セキュリティリーダである T 課長は，これらの施策に係る情報セキュリティリスクアセスメントの実施とリスク対応が必要と考え，S 課長に相談したところ，表 3 のようなアドバイスを受けた。

表3　S課長のアドバイス

施策	アドバイス
個人向け通信販売	・通信販売の開始によって，②適用される法令への対応と，それに伴うX社ISMS文書の見直しが必要になる。 ・クレジットカードによる決済への対応として，次の二つの案が考えられる。 案1　X社Webサイトを改修し，X社でクレジットカード決済を行う。［　a　］への準拠が必要になるので，X社ISMSに管理策を追加する。 案2　通信販売は行うが，X社としてクレジットカード情報を非保持化する。クレジットカード決済には外部のオンラインショッピングサイトを利用する。
X社Webサイトの改修	（省略）
SNSによる情報提供	・X社ISMSにおいては，業務用PCでのSNSの利用が禁止されている。業務でSNSを利用するのであれば，SNSのリスクについて検討した上で，X社ISMS文書を見直す必要がある。

S課長のアドバイスを受け，T課長は個人向け通信販売については，案2を採用し，外部のオンラインショッピングサイトを利用するのがよいと考えた。利用するシステムの詳細が固まった後に改めて情報セキュリティリスクアセスメントを行い，ISMS-WGに確認してもらうことにした。

次に，S課長とT課長はSNSを利用した情報提供に起因するリスクについて検討することにした。S課長は，T課長に次のリスクを説明した。

リスク1　X社の従業員が，X社公式アカウントを用いてX社の信用及び評判を低下させるような投稿を行う。

リスク2　第三者がX社公式アカウントを装い，X社の信用及び評判を低下させるような投稿を行う。

リスク3　第三者がX社公式アカウントを乗っ取り，X社の信用及び評判を低下させるような投稿を行う。

S課長の説明を聞いたT課長は，機械営業部だけでこれらのリスクに対応することは困難と判断した。そこで，SNSを利用した情報提供に起因するリスクについては，全社的な対策を立案するようS課長に依頼した。

また，S課長は，業務外でのSNSの個人利用についても，次のようなリスクがあることをT課長に説明した。

リスク 4　X 社の従業員が，X 社の信用及び評判を損なうような不用意な投稿を行う。

リスク 5　X 社の従業員が，その投稿から③X 社及び従業員の情報を攻撃者に推測され，X 社に対する標的型攻撃の手掛かりにされるような不用意な投稿を行う。

これらのリスクを踏まえ，T 課長は，業務外での SNS の個人利用についても，従業員向けに何らかの指針を示すのがよいのではないかと S 課長に提言した。S 課長は，SNS の利用に関するルールを立案し，ISMS-WG で検討することにした。

〔SNS の利用に関する情報セキュリティ対策〕

数日後，S 課長は X 社公式アカウントの運用に関する情報セキュリティ対策の案を作成した。その内容を表 4 に示す。

表 4　X 社公式アカウントの運用に関する情報セキュリティ対策（案）

項目	内容
利用目的の限定	X 社公式アカウントの利用は，製品情報の発信，お客様からの問合せへの返信などの業務目的に限定する。
発信者の限定	X 社公式アカウントを利用する担当者（以下，SNS 担当者という）を限定する。
X 社からの公式な情報発信であることの明示	X 社公式アカウントについて，次の事項を実施する。 ・ b1 ・ b2 ・ b3
アカウント乗っ取りの防止	SNS 担当者に対して，次の事項を徹底させる。 ・ c1 ・ c2 ・ c3

また，S 課長は，SNS の個人利用に関する指針を策定し，12 月に実施する従業員向け情報セキュリティ教育の内容に含めることにした。SNS の個人利用を一律に禁止することは適切でないので，この指針では，法令及び雇用契約上の要求事項の観点から従業員が順守すべき事項と，SNS の利用に当たって従業員が実施することが推奨される事項に分けて記載することにした。その概要を表 5 に示す。

表5　SNSの個人利用に関する指針（概要）

項目	内容
順守すべき事項	SNSの個人利用においては，次の事項を順守する。 ・ d1 ・ d2 ・ d3 （省略）
推奨される事項	SNSの個人利用においては，次の事項を実施することが推奨される。 ・ e1 ・ e2 ・ e3 （省略）

X社公式アカウントの運用に関する情報セキュリティ対策及びSNSの個人利用に関する指針は，ISMS-WGでの検討を経て情報セキュリティ委員会において承認された。

〔オンラインショッピングサイトの利用〕

機械営業部は，大手通信販売業者であるZ社のオンラインショッピングサイト（以下，Zショップという）を利用して個人向けに3DP及びオプション品を販売することにした。Zショップでは，消費者向けサイト以外にも各出品者用にポータルサイトを提供している。

X社には，Z社からX社専用のポータルサイト（以下，X社ポータルという）へのアクセス権が付与され，X社ポータルを利用する業務担当者用アカウントを追加又は削除可能な管理者用アカウントが一つ設定された。この管理者用アカウントでは，X社ポータルの他の機能を利用する個々の業務担当者用アカウントの管理だけを行うことにした。X社ポータルで業務担当者用アカウントを追加すると，その業務担当者のメールアドレスに対して電子メールが送信され，初期パスワードの変更が促される。

X社ポータルで利用可能な機能とその内容を表6に示す。

表6　X社ポータルの機能と内容

機能	内容
商品登録	・Zショップに出品する商品の情報の登録，修正及び削除
在庫管理	・Zショップに出品した商品の在庫数及び販売価格の管理
受注管理	・Zショップで受注した商品の納期，配送先の氏名，住所などの受注情報の確認 ・受注情報のCSV形式でのダウンロード ・購入者への発送通知
売上管理	・取引ごとの売上情報の確認 ・Z社に支払う手数料及びZ社からの入金に関する情報（以下，決済情報という）の確認 ・売上情報及び決済情報のCSV形式でのダウンロード
アカウント管理	・X社ポータルにアクセスできる別の業務担当者用アカウントの追加 ・システム上の役割（以下，ロールという）の登録，削除 ・X社ポータルの機能と次のいずれかの利用権限の組合せの，ロールへの付与 編集：情報の閲覧，ダウンロード及び編集ができる。 閲覧：情報の閲覧はできるがダウンロードと編集はできない。 ・アカウントへのロールの設定

機械営業部では，X社ポータルで表7に示すロールを新たに登録することにした。

表7　X社ポータルに新たに登録するロールと主な作業

新たなロール	X社ポータルで行う主な作業
商品担当者ロール	・出品する商品の情報を管理する。 ・在庫状況を反映する。
発送担当者ロール	・受注情報をダウンロードし，それに基づく商品発送を行う。 ・発送が完了したら，発送通知を行う。
経理担当者ロール	・売上情報及び決済情報をダウンロードし，X社の会計システムに入力する。

アカウントにロールを設定された業務担当者は，自分の業務用PCでX社ポータルにアクセスし，利用権限を付与された機能を利用して作業を行う。

機械営業部では，表6及び表7を基に，各ロールに付与する利用権限を検討することにした。その案を表8に示す。

表8　各ロールに付与する利用権限（案）

機能／ロール	商品登録	在庫管理	受注管理	売上管理	アカウント管理
X社ポータル管理者ロール[1)]	◎	◎	◎	◎	◎
商品担当者ロール	◎	◎	×	×	×
発送担当者ロール	○	◎	◎	×	×
経理担当者ロール	×	○	○	◎	×

注記　◎は編集の利用権限が付与されることを，○は閲覧の利用権限が付与されることを，×は利用権限が付与されないことを示す。

注[1)]　あらかじめ管理者用アカウントに設定されている。

X 社 ISMS では，今回のように業務を大きく変更する場合は，情報セキュリティリスクアセスメントを実施し，リスク対応を行うことになっている。そこで，この案について，T 課長が S 課長に相談したところ，次の指摘を受けた。

指摘 1　発送担当者ロールを割り当てられた業務担当者は業務で購入者情報を扱うので，その業務担当者の業務用 PC に購入者情報が蓄積されるおそれがあり，対策が必要である。

指摘 2　X 社ポータル管理者ロールの利用権限が過大であり，不正が起こるおそれがある。X 社ポータル管理者ロールの利用権限を分割すべきである。

これらの指摘を受け，T 課長は，指摘 1 については，発送担当者ロールを割り当てられた業務担当者に対して業務用 PC に蓄積された購入者情報の利用後の削除を徹底させるとともに，購入者情報が蓄積されていないことを上長に定期的に点検させることにした。また，指摘 2 については，表 8 を見直して X 社ポータル管理者ロールの利用はやめるとともに，アカウント管理を含む X 社ポータルの各機能の利用状況のモニタリングを行うために，新たなロールを追加することにした。追加する新たなロールとそのロールに付与する利用権限の案を，表 9 に示す。

表 9　追加する新たなロールとそのロールに付与する利用権限（案）

機能 / ロール	商品登録	在庫管理	受注管理	売上管理	アカウント管理
アカウント管理ロール	（省略）			f1	f2
モニタリングロール				g1	g2

これらの案は ISMS-WG で検討され，情報セキュリティ委員会の承認を得て，Z ショップで 3DP の販売が開始されることになった。

その後，Z ショップからの新製品の販売は順調に進んでいる。

設問１　表１中の下線①について，該当する作業を三つ，解答群の中から選べ。

解答群

ア　新たに追加された情報資産の名称と管理責任者を記載する。

イ　記載された情報資産の重要度が適切であるか確認する。

ウ　記載された情報資産のリスクを低減する。

エ　情報資産目録に対するアクセス権を設定する。

オ　情報資産目録の情報セキュリティパフォーマンス及びX社ISMSの有効性を評価する。

カ　廃棄された情報資産を情報資産目録から削除する。

設問２　〔販路拡大のための施策〕について，(1)～(3)に答えよ。

(1)　表3中の下線②について，適用される法令，及び見直しが必要なX社ISMS文書の組合せはどれか。解答群のうち，最も適切なものを選べ。

解答群

	法令	X社ISMS文書
ア	個人情報の保護に関する法律	情報セキュリティ方針
イ	個人情報の保護に関する法律	適用宣言書
ウ	個人情報の保護に関する法律	適用法規制一覧
エ	電気通信事業法	情報セキュリティ方針
オ	電気通信事業法	適用宣言書
カ	電気通信事業法	適用法規制一覧
キ	特定商取引に関する法律	情報セキュリティ方針
ク	特定商取引に関する法律	適用宣言書
ケ	特定商取引に関する法律	適用法規制一覧

(2) 表3中の［ a ］に入れる適切な字句を，解答群の中から選べ。

aに関する解答群

ア JIS Q 15001　　イ JIS Q 20000

ウ JIS Q 27017　　エ NIST SP 800-171

オ PCI DSS　　カ 情報セキュリティサービス基準

(3) 本文中の下線③に当てはまる攻撃手法はどれか。解答群のうち，最も適切なものを選べ。

解答群

ア キーロガー　　イ クリプトジャッキング

ウ サイドチャネル攻撃　　エ セッション固定攻撃

オ 総当たり攻撃　　カ ソーシャルエンジニアリング

キ ディレクトリトラバーサル　　ク パスワードリスト攻撃

ケ バッファオーバフロー攻撃　　コ レインボー攻撃

設問3　〔SNS の利用に関する情報セキュリティ対策〕について，(1) ～ (4) に答えよ。

(1)　表 4 中の［ b1 ］～［ b3 ］に入れる，次の (i) ～ (v) の組合せはどれか。b に関する解答群のうち，最も適切なものを選べ。

(i)　SNS アカウントのプロフィールにおいて，X 社のアカウントであることを明示する。

(ii)　SNS 担当者の個人アカウントと X 社公式アカウントとの相互フォローを行う。

(iii)　SNS の提供業者に審査を申請し，認証済みアカウントであることを表示してもらう。

(iv)　X 社 Web サイトに，X 社公式アカウントのページへのリンク及び X 社公式アカウントの運用方針を明示する。

(v)　X 社のメールサーバで，SPF（Sender Policy Framework）を用いた送信ドメイン認証を行う。

b に関する解答群

	b1	b2	b3
ア	(i)	(ii)	(iii)
イ	(i)	(ii)	(iv)
ウ	(i)	(ii)	(v)
エ	(i)	(iii)	(iv)
オ	(i)	(iii)	(v)
カ	(i)	(iv)	(v)
キ	(ii)	(iii)	(iv)
ク	(ii)	(iii)	(v)
ケ	(ii)	(iv)	(v)
コ	(iii)	(iv)	(v)

(2) 表 4 中の [c1] ～ [c3] に入れる，次の (i) ～ (v) の組合せはどれか。c に関する解答群のうち，最も適切なものを選べ。

(i) X 社公式アカウントによる投稿への，利用者からのアクセス状況をレビューする。

(ii) X 社公式アカウントのパスワードを他のサービスのものと共用しない。

(iii) X 社公式アカウントの利用者 ID を広く宣伝し，認知度を高める。

(iv) X 社公式アカウントへの投稿については，社内の定められた業務用 PC からだけ行う。

(v) X 社公式アカウントへのログインには，記憶を利用した認証と所持しているものを利用した認証を併用する。

c に関する解答群

	c1	c2	c3
ア	(i)	(ii)	(iii)
イ	(i)	(ii)	(iv)
ウ	(i)	(ii)	(v)
エ	(i)	(iii)	(iv)
オ	(i)	(iii)	(v)
カ	(i)	(iv)	(v)
キ	(ii)	(iii)	(iv)
ク	(ii)	(iii)	(v)
ケ	(ii)	(iv)	(v)
コ	(iii)	(iv)	(v)

(3) 表 5 中の [d1] ～ [d3] に入れる，次の (i) ～ (v) の組合せはどれか。d に関する解答群のうち，最も適切なものを選べ。

(i) 業務上の守秘義務に反する投稿を行わない。

(ii) 業務用 PC では SNS の個人利用を行わない。

(iii) 自分の投稿は X 社の公式見解である旨を SNS のプロフィールに明示する。

(iv) 投稿に当たっては，著作権，肖像権などの他人の権利の侵害に注意する。

(v) 取引先の従業員とは SNS 上での私的な交流は行わない。

d に関する解答群

	d1	d2	d3
ア	(i)	(ii)	(iii)
イ	(i)	(ii)	(iv)
ウ	(i)	(ii)	(v)
エ	(i)	(iii)	(iv)
オ	(i)	(iii)	(v)
カ	(i)	(iv)	(v)
キ	(ii)	(iii)	(iv)
ク	(ii)	(iii)	(v)
ケ	(ii)	(iv)	(v)
コ	(iii)	(iv)	(v)

(4) 表 5 中の [e1] ～ [e3] に入れる，次の (i) ～ (v) の組合せはどれか。e に関する解答群のうち，最も適切なものを選べ。

(i) SNS 上で投稿を削除しても，その投稿が拡散されてしまう可能性があることに留意して投稿する。

(ii) SNS を利用する個人所有の端末について，適切な物理的及び技術的対策を実施する。

(iii) 投稿に URL を含めるときは，URL 短縮サービスを利用する。

(iv) 面識のなかった人から SNS を通じて“友達”関係の形成など交流の申出を受けた場合には，積極的に受諾し，人間関係の拡大に努める。

(v) 利用する SNS ごとに，発信する情報の公開範囲を適切に設定する。

e に関する解答群

	e1	e2	e3
ア	(i)	(ii)	(iii)
イ	(i)	(ii)	(iv)
ウ	(i)	(ii)	(v)
エ	(i)	(iii)	(iv)
オ	(i)	(iii)	(v)
カ	(i)	(iv)	(v)
キ	(ii)	(iii)	(iv)
ク	(ii)	(iii)	(v)
ケ	(ii)	(iv)	(v)
コ	(iii)	(iv)	(v)

設問4　〔オンラインショッピングサイトの利用〕について，(1)，(2) に答えよ。

(1)　表 9 中の［ f1 ］，［ f2 ］に入れる記号の適切な組合せを，f に関する解答群の中から選べ。ここで，◎，○及び×は表 8 の注記と同一である。

f に関する解答群

	f1	f2
ア	◎	◎
イ	◎	○
ウ	◎	×
エ	○	◎
オ	○	○
カ	○	×
キ	×	◎
ク	×	○
ケ	×	×

(2)　表 9 中の［ g1 ］，［ g2 ］に入れる記号の適切な組合せを，g に関する解答群の中から選べ。ここで，◎，○及び×は表 8 の注記と同一である。

g に関する解答群

	g1	g2
ア	◎	◎
イ	◎	○
ウ	◎	×
エ	○	◎
オ	○	○
カ	○	×
キ	×	◎
ク	×	○
ケ	×	×